Technical Cybersecurity

NMAP Lab Configuration

We’ve downloaded and installed. Now to network.

Step 2: Networking

Isolation

- You will want to run exploitable systems in isolation
- VMs need to be networked so they can see each other

Host v. Target VMs

- Target VMs have exploitable flaws, we don’t want to update these
  - …do not need internet access
- Host VMs (ones we work with) we will need to update occasionally
  - …will need occasional internet access

Network Configuration

Use two network adapters for Host VMs

- One is shared with the host, allows external access
- The other is private, shared only with the host system

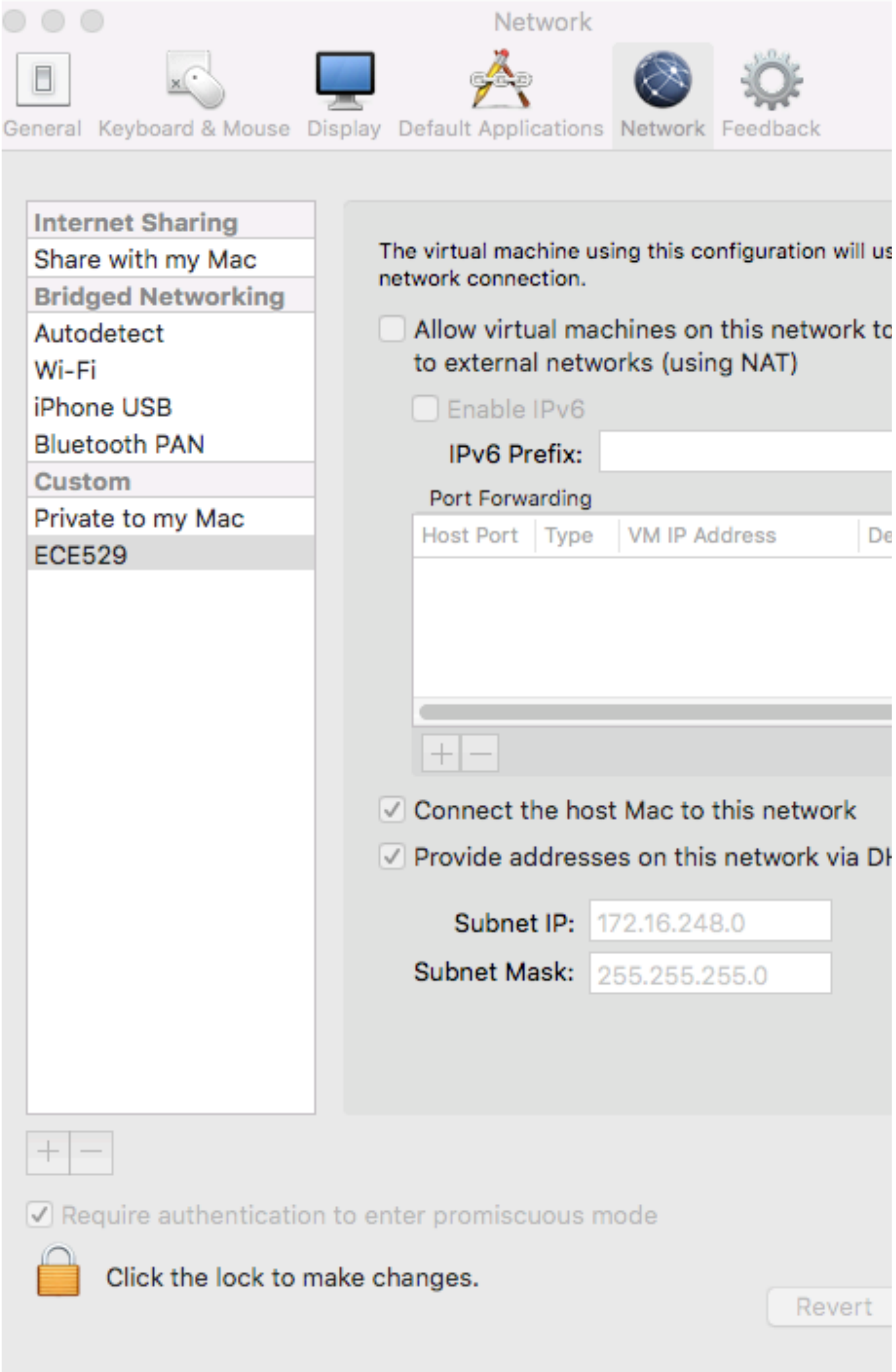
Use one network adapter for Target VMs

- This should be private, no internet access
- If images install with two, deactivate one

VMWare Network Config

Create a private network

- I've named it ECE529
- Enable local connections
- Enable DHCP
- DO NOT enable NAT



Internet Sharing
Share with my Mac
Bridged Networking
Autodetect
Wi-Fi
iPhone USB
Bluetooth PAN
Custom
Private to my Mac
ECE529

The virtual machine using this configuration will us
network connection.

□ Allow virtual machines on this network to
to external networks (using NAT)

□ Enable IPv6

IPv6 Prefix:

Port Forwarding

Host Port	Type	VM IP Address	De

☑ Connect the host Mac to this network

☑ Provide addresses on this network via DH

Subnet IP: 172.16.248.0

Subnet Mask: 255.255.255.0

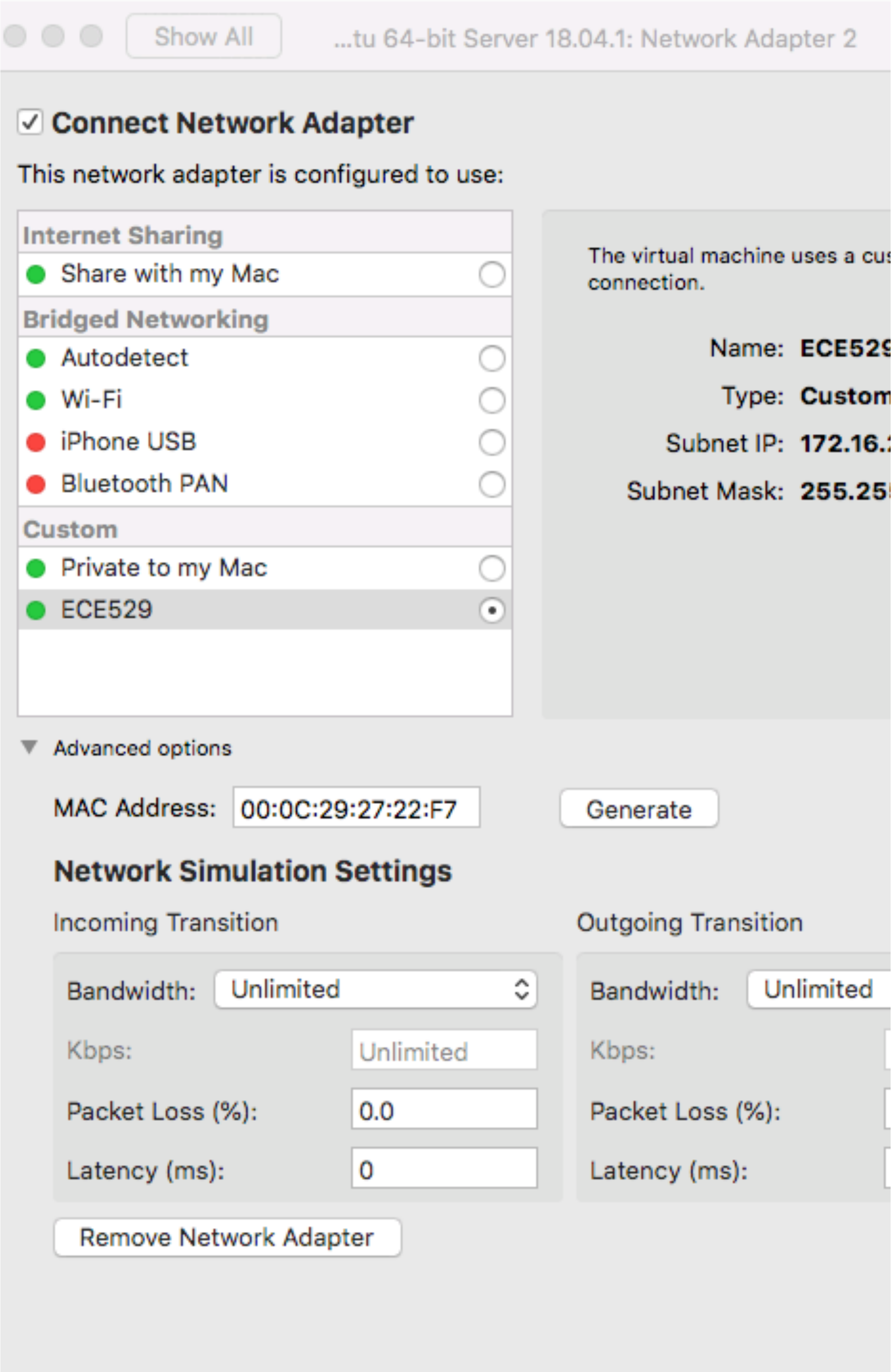
☑ Require authentication to enter promiscuous mode

Click the lock to make changes.

Metasploitable

Remove Network Adapter 2

- VM must be shutdown to remove adapters
- Settings -> Network Adapter 2 -> Advanced Options
- Remove Network Adapter is as the bottom



☑ **Connect Network Adapter**

This network adapter is configured to use:

Internet Sharing

- 🟢 Share with my Mac ○

Bridged Networking

- 🟢 Autodetect ○
- 🟢 Wi-Fi ○
- 🔴 iPhone USB ○
- 🔴 Bluetooth PAN ○

Custom

- 🟢 Private to my Mac ○
- 🟢 ECE529 ●

The virtual machine uses a cus
connection.

Name: **ECE529**
Type: **Custom**
Subnet IP: **172.16.**
Subnet Mask: **255.25**

▼ Advanced options

MAC Address: 00:0C:29:27:22:F7 Generate

Network Simulation Settings

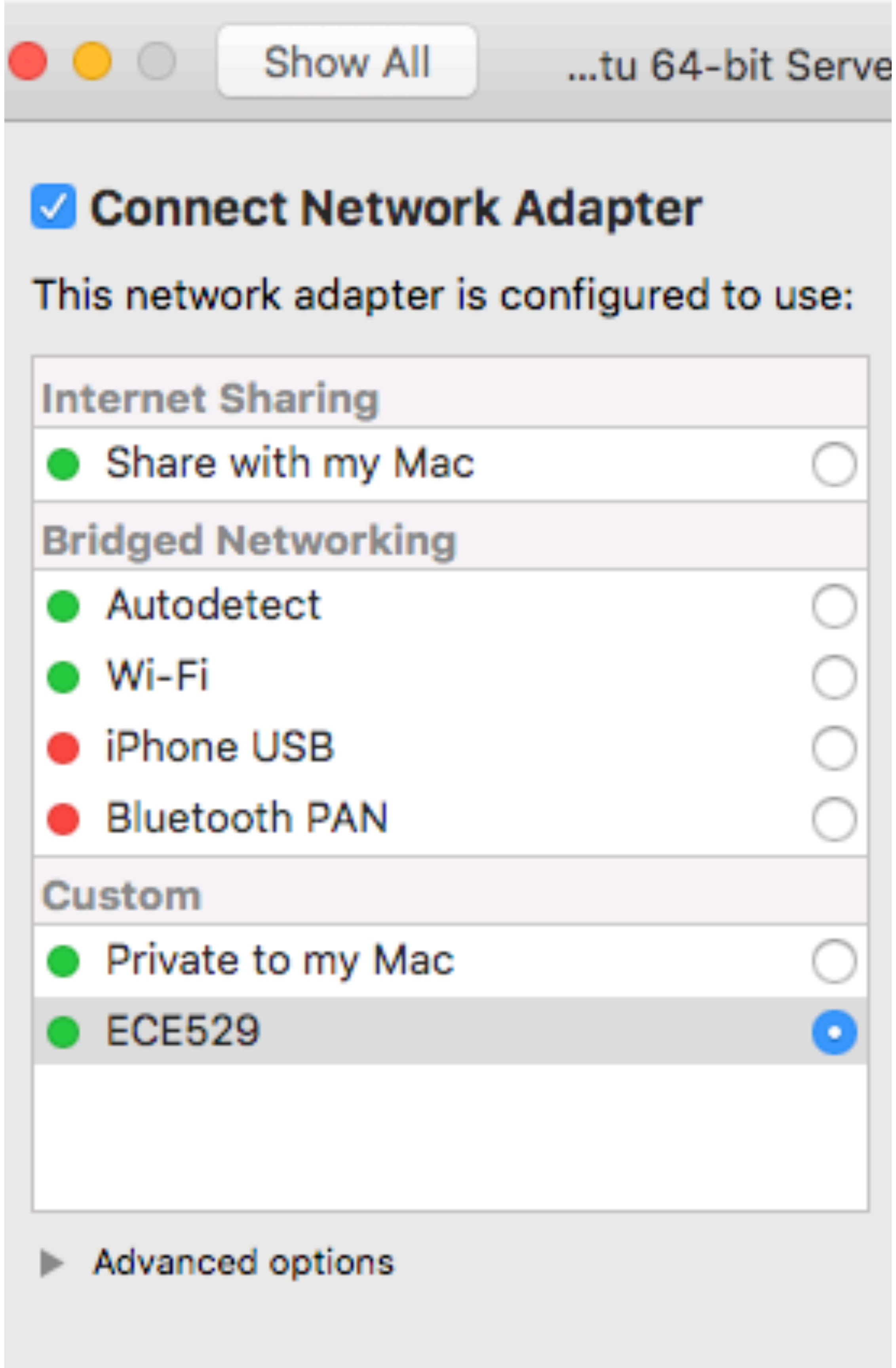
Incoming Transition		Outgoing Transition	
Bandwidth:	Unlimited	Bandwidth:	Unlimited
Kbps:	Unlimited	Kbps:	
Packet Loss (%):	0.0	Packet Loss (%):	
Latency (ms):	0	Latency (ms):	

Remove Network Adapter

pivot/kali

UBUNTU LTS

- Two network adapters are fine
- One can share with host
- Other attached to ECE529 network
- Kali should be configured in same way



☑ Connect Network Adapter

This network adapter is configured to use:

Internet Sharing
- 🟢 Share with my Mac ○

Bridged Networking
- 🟢 Autodetect ○
- 🟢 Wi-Fi ○
- 🔴 iPhone USB ○
- 🔴 Bluetooth PAN ○

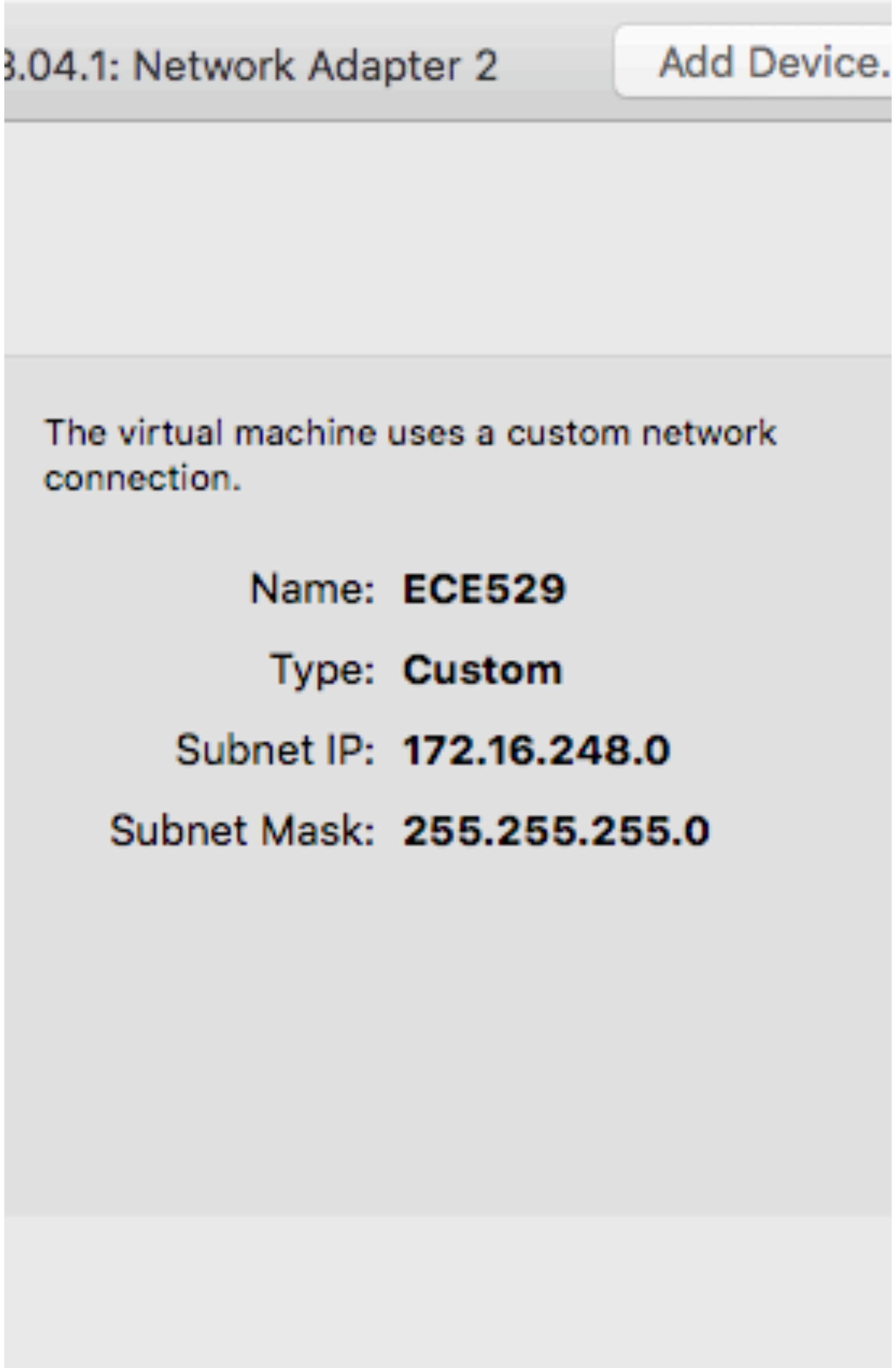
Custom
- 🟢 Private to my Mac ○
- 🟢 ECE529 ●

▶ Advanced options

Boot them up!

LOG IN AT CONSOLE

- Look at ECE network from network adapter (your subnet IP might differ)
- Ping hosts to check for connectivity
- Can you ping?



The virtual machine uses a custom network connection.

Name: ECE529

Type: Custom

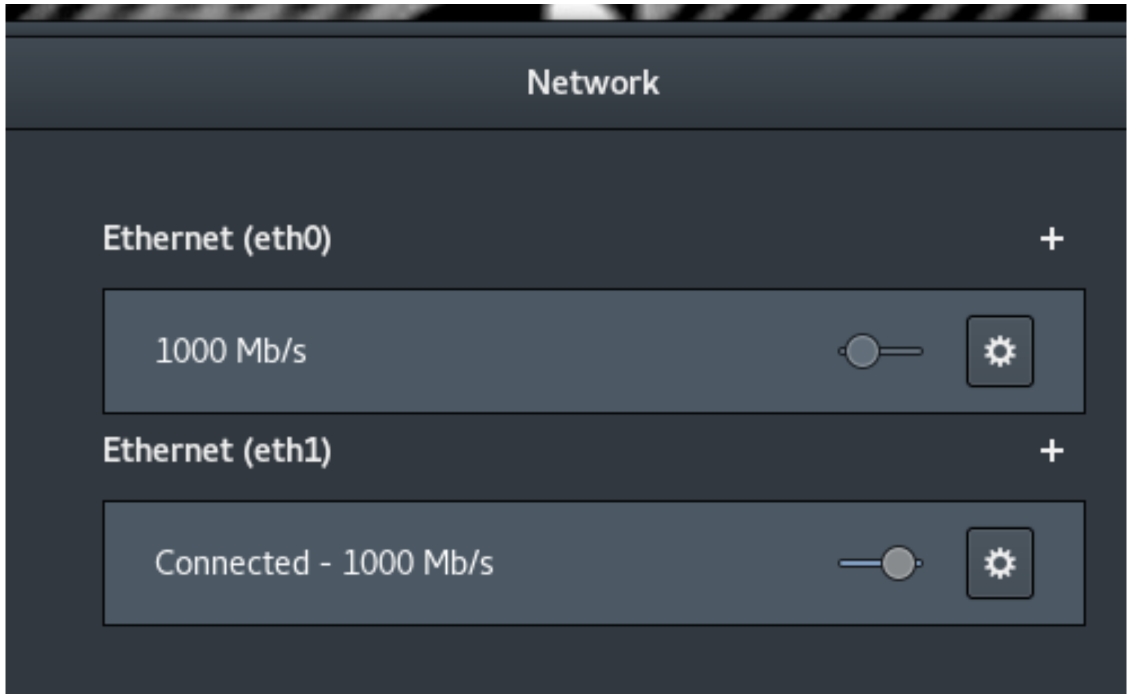
Subnet IP: 172.16.248.0

Subnet Mask: 255.255.255.0

Kali: Network Config

External Network

- You may need to switch on external network on your Kali VM
- You can turn the external network on, but the lab network will shut down when you do, and vice versa
- Settings -> Network
- Here, I have the lab active



Network

Ethernet (eth0)

1000 Mb/s

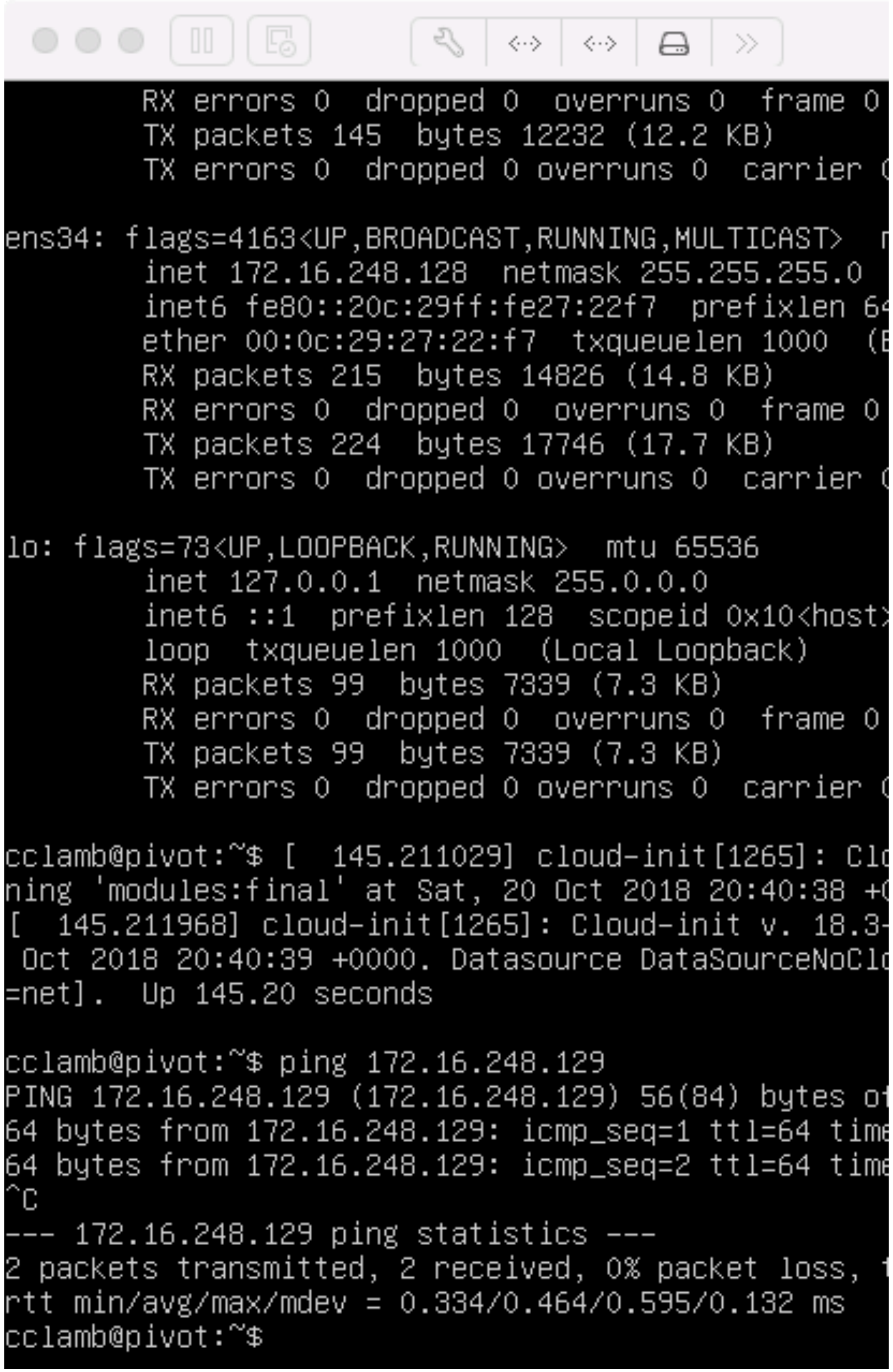
Ethernet (eth1)

Connected - 1000 Mb/s

Other tricks

SSH

- ssh to your hosts. Don’t use the VMWare console.
- Learn how to use a terminal multiplexer (TMUX or SCREEN)



```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 145  bytes 12232 (12.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier

ens34: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
        inet 172.16.248.128  netmask 255.255.255.0
        inet6 fe80::20c:29ff:fe27:22f7  prefixlen 6
        ether 00:0c:29:27:22:f7  txqueuelen 1000  (
        RX packets 215  bytes 14826 (14.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 224  bytes 17746 (17.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 99  bytes 7339 (7.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 99  bytes 7339 (7.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier

cclamb@pivot:~$ [  145.211029] cloud-init[1265]: Clo
ning 'modules:final' at Sat, 20 Oct 2018 20:40:38 +
[  145.211968] cloud-init[1265]: Cloud-init v. 18.3
 Oct 2018 20:40:39 +0000. Datasource DataSourceNoCl
=net].  Up 145.20 seconds

cclamb@pivot:~$ ping 172.16.248.129
PING 172.16.248.129 (172.16.248.129) 56(84) bytes of
64 bytes from 172.16.248.129: icmp_seq=1 ttl=64 time
64 bytes from 172.16.248.129: icmp_seq=2 ttl=64 time
^C
--- 172.16.248.129 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss,
rtt min/avg/max/mdev = 0.334/0.464/0.595/0.132 ms
cclamb@pivot:~$
```

You should have three VMs (kali, ubuntu, and metasploitable). Now we’ll scan.